STATEMENT

OF

MARK M. MACCARTHY

ON BEHALF OF

VISA U.S.A. INC.

BEFORE THE

SUBCOMMITTEE ON

FINANCE AND TAX

OF THE

COMMITTEE ON SMALL BUSINESS

UNITED STATES HOUSE OF REPRESENTATIVES

Data Security: Small Business Perspectives

June 6, 2007

Chairwoman Bean and Members of the Subcommittee, my name is Mark MacCarthy. I am the Senior Vice President for Public Policy for Visa U.S.A. Inc. ("Visa"). Visa appreciates the opportunity to address the important issues raised by today's hearing on data security and small businesses.

The Visa Payment System, of which Visa U.S.A. is a part, is a leading consumer payment system, and plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of data security and its impact on small businesses. As the leading consumer e-commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect the customer information of our members.

Visa has substantial incentives to maintain and promote strong security measures to protect customer information. Cardholder security is never just an afterthought in the transaction cycle at Visa. For Visa, it's about trust. Our goal is to protect consumers, merchants and our members from fraud by preventing fraud from occurring in the first place. This commitment to fighting fraud extends to Visa's Zero Liability policy, which protects Visa cardholders from any liability for fraudulent purchases. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs primarily are in the form of direct dollar losses from credit that

will not be repaid. They also include card replacement costs, fraud monitoring costs and incremental customer service costs. In order to protect our members from these costs, Visa aggressively protects their customer information.

Visa's Information Security Programs

Visa employs a multi-faceted approach to combat account fraud and identity theft. Visa has implemented a comprehensive and aggressive customer information security program known as the Cardholder Information Security Program ("CISP"). This security program applies to all entities, including merchants, that store, process, transmit or hold Visa cardholder data, and covers entities that operate through brick-and-mortar stores, mail and telephone order centers and the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP not only includes data security standards, but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

In addition, Visa has successfully integrated CISP into the common set of data security requirements used by various credit card organizations without diluting the substantive measures for information security already developed in CISP. Visa supports this common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("PCI Standard"). To help accelerate compliance with the PCI Standard and to eliminate the storage of sensitive card data, Visa launched the Visa PCI Compliance Acceleration Program to provide acquirers with financial incentives for their merchants' validation of compliance and to expand monetary fines for the storage of prohibited data and noncompliance with the PCI Standard.

Visa also provides sophisticated neural networks that flag unusual spending patterns for fraud that enable our members to block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institutions and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigating and evaluating the need to reissue cards.

Similarly, Visa has implemented a new Account Data Compromise Recovery ("ADCR") process to resolve disputes related to account compromises that have been linked to magnetic strip-read counterfeit fraud. The ADCR process is used exclusively when magnetic strip data is determined to be compromised. Once a merchant notifies its acquirer of an account compromise, the acquirer sends the stolen card account numbers directly to Visa's Compromised Account Management System. Visa then validates that an account compromise has occurred and notifies issuers about the compromised accounts. Affected issuers can monitor or close the compromised accounts or block transactions that are attempted on such accounts.

Visa has implemented a number of other security measures designed to detect and prevent particular fraudulent transactions:

- Visa's Address Verification Service matches shipping and billing addresses and other information to confirm that a transaction is valid.
- Visa maintains an exception file comprised of a worldwide database of account numbers of lost or stolen cards and other cards that issuers have designated for confiscation or other special handling. All transactions

processed through the Visa system have the account numbers checked against this exception file.

- The Cardholder Verification Value ("CVV") is a unique three-digit code included in the magnetic strip located on the back of all Visa cards. The CVV is electronically checked during the authorization process for card-present transactions to ensure that a valid card is present.

- The CVV2 is a unique three-digit code printed on the signature strip on the back of all Visa cards. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants or telephone merchants conducting transactions when the card is not present can verify that their customers have the actual card by requesting the customer to provide the CVV2 number.

- Verified by Visa both protects customers and allows merchants, including all kinds of small businesses, to avoid charge-back costs in online transactions by having cardholders authenticate their identities while shopping online. Its password protection reduces the potential for fraud over the Internet.

- Advance Authorization provides an instantaneous analysis of the potential for fraud at the time of a transaction.

As a result of these strong security measures, fraud conducted within the Visa system ranges from five to six cents for every $100 of transactions.

Visa also has security programs that focus specifically on small businesses, which account for the vast majority of the more than 6 million merchants that accept Visa cards in the U.S. To promote sound security practices for small merchants, Visa has:

- Conducted numerous webinars, conference calls and other training programs targeted at small merchants.
- Developed the Payment Application Best Practices to promote the use of secure payment applications that do not cause the storage of sensitive data.
- Distributed a list of vulnerable payment applications that have been found to cause the storage of sensitive data.
- Published a number of security alerts and articles to promptly notify acquirers and merchants of the latest security vulnerabilities.

In addition, Visa and the U.S. Chamber of Commerce recently conducted a 12-city nationwide data security education campaign to involve both the payments industry and merchants in the fight to protect cardholder information and reduce fraud. Visa believes that all parties that participate in the payment system, including small businesses, share responsibility to protect cardholder information.

Pending Data Security Legislation

Visa has not taken a position on specific data security legislation that is pending. In general, we favor reasonable risk-based security and notification requirements that would apply to all entities that have sensitive customer information. However, these standards should take into consideration the size and complexity of an entity's business, as well as the nature and scope of its business activities. As noted above, Visa believes

that all participants in the payment system, including small businesses, share responsibility to protect cardholder information. Nonetheless, most small businesses often do not engage in practices, such as storing credit card transaction data, that create incentives for thieves to attack their systems. Visa's validation requirements recognize this fact by adopting a tiered approach that allows small businesses to self certify their compliance with the PCI Standard.

We also believe that security and notification standards should be consistently applied nationwide to avoid a clash of conflicting state laws in this area. Finally, we favor stronger penalties for identity theft and additional resources for state and local law enforcement to combat identity theft.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.